Standards Approved by Internet Standards Committee

This document is a summary of those standards, policies and guidelines passed by the Internet Standards Committee. Any standards or policies that appear in this document have also been approved by the Internet Steering Committee and apply to all areas of CDC and ATSDR.

It is intended for use by CDC/ATSDR as a consolidated list of all approved Internet standards, policies and guidelines. The order of documents is chronological.

Table of Contents

94.1: FTP Server

At the 9/1/94 meeting the Committee provided the following guidance to the Steering Committee: AAnonymous FTP will be freely allowed for downloads from CDC. There will be no anonymous FTP for uploads to CDC. Exceptions to this last standard need to brought to this standards committee for review.@ The Excellence in Science Committee developed two policy statements deriving from guidance provided:

94.1.A: Policy On Anonymous FTP Use

Anonymous FTP may be used for the provision over the Internet of documents, files and datasets which have been officially cleared for public distribution. Documents and datasets previously cleared for publication or public distribution may be provided over the Internet without further clearance.

In no case will Anonymous FTP upload of material to CDC/ATSDR be allowed. If collection or receipt of materials over the Internet is needed then Internet mail facilities should be used.

94.1.B: Policy On Internet Disclaimers

Materials provided to the public over the Internet will include or be accompanied by the following disclaimer:

"This material is provided by _____ [organization name] which is a sub-unit of CDC/ATSDR. I has been cleared for public distribution by CDC/ATSDR and will be authentic if gotten from _____ [Internet address, listserv address, URL, etc]. "

This disclaimer may be incorporated into the document, file or dataset or may be included in an additional document or file clearly associated with document(s), file(s), or dataset(s). If a single disclaimer is applied to the contents of an entire disk directory it should be as a file named disclaim.txt.

The Committee discussed the above policy statements at the 9/13/94 meeting and sent back to the Steering Committee the following comment: AThe majority opinion was to endorse the Steering Committee recommendation, with the caveat that they explicitly provide a mechanism for exceptions to the Ano anonymous FTP upload@ rule be brought to the standards committee for review and possible exception granting. Roy Ing (NCEH) disagrees with this policy and believes that CDC should offer anonymous FTP upload services to selected servers. His exception is noted and forwarded to the Steering Committee for review.@

94.2: Accounts

At 9/13/94 meeting the Committee passed the following standards for user accounts on the Internet:

> **94.2.A:** Inside the Firewall. The Committee felt that there should be a one-to-one correspondence between individuals and accounts and that CDC should assign passwords. There will be no Aguest accounts.@
>
> **94.2.B:** Outside the Firewall. In general, the inside the firewall rule would apply. There would be exceptions granted by the Standards Committee for special needs. Variations on the one-to-one correspondence rule might be granted in the case of a need to gather comments on outstanding proposals or to solicit feedback on CDC programs. These semi-anonymous accounts might be time-limited, be set up on a special machine, or have variable password standards. Each would be handled on a case-by-case basis.

94.3: Document Formats

At the 9/27/94 meeting, the Committee suggested the following standard for the format of documents placed in Internet:

> "For CDC documents to be distributed over the Internet which are intended for viewing (as opposed to data files or programs), there should be at least one version available in either ASCII, PDF, or HTML, for which there are no-cost readers. This is not intended to restrict additional distribution in formats that require a commercial product for viewing (e.g., WordPerfect), or printing (HPGL, Postscript)."

Comments to this standard were requested from the Committee, but none were received.

94.4: LISTSERV

Note: This approved standard was essentially superseded by the Sponsored Discussion Forum (96.2).

At the 11/8/94 meeting of the Committee the following standard regarding LISTSERV service was approved:

> **94.4.A:** LISTSERVs are a standard part of the Internet and support CDC's mission; they aid our work with our partners in prevention in both the US and abroad through improved communication. LISTSERVice should be approved for use to support any and all of the tools of prevention, including but not limited to activities related to surveillance, health statistics, epidemiology, laboratory science, behavioral risk reduction, technology transfer, prevention strategies and programs and health communication.
>
> **94.4.B:** Approval of LISTSERV applications belongs to the CIO requesting the service, and no application can be implemented prior to clearance. Each CIO should document its clearance process for this service to the Excellence in Science Committee.
>
> **94.4.C:** LISTSERVice is a centralized activity provided through IRMO at this time. CIOs can establish and administer their own LISTSERVers.

94.5: Home Page

The Home Page Subcommittee was formed at the 9/1/94 meeting and reported on various aspects of the developed of Home Page standards and an interim CDC Home Page at all subsequent meetings. At the 11/8/94 meeting the standards were adopted and an interim Home Page was accepted.

At the 9/1/94 meeting the following Home Page Issues were approved by the Committee:

94.5.A: There will be a CDC home page.

94.5.B: CIOs are free to develop subsidiary home pages that are organized either along organizational or subject matter lines.

94.5.C: There will be a way to move directly back from any of these subsidiary home pages to the CDC home page, whether this is from an organizational or subject matter entry point that has been advertised.

While no specific vote appears in the minutes, implicate in the third item was that the initial CIO Home Pages and other immediately subsidiary Home Pages to the CDC Home Page would adhere to the standards set for the CDC Home Page. Home Pages subsidiary to the CIO or other subsidiary Home Pages did not have to adhere to the CDC Home Page Standard. The intent was to provide a uniform organizational look.

94.5.D: The formal Home Page Standards approved by the Committee at the 11/8/94 meeting are as follows:

94.5.D (1): Identifier (at top of page): 580 (maximum width) x 100± pixels
Width may differ from home page to home page.

The resolution of photographs is too variable (depending on the viewing monitor) for photographs to be useful as identifiers.

The home page should appear promptly.
The size of the GIF file affects transmission time.

For any graphic on a home page, use the ALT option of HTML and provide a text substitute for viewing on nongraphics terminals.

94.5.D (2): Font: Times Roman
All text outside graphic identifier: Use upper-and lowercase (not all caps).

Welcome: If not using a graphic identifier, provide a welcome, using header 1 attribute.

Vision or mission: Using attributes, define as header 2 (optional for CIO home page).

Major links: Times Roman 12 (bold)
All other text: Times Roman 12 (no bold or italics)
Internet address: Use address attribute.

Use the HTML Title attribute to identify a home page.

We cannot, of course, control the font in which users view the home page. Our recommendations are for design and optimal viewing.

94.5.D (3): Migration points: balls or bullets (rather than icons)

94.5.D (4): "Return to CDC home page" icon: to appear on all CIO home pages

94.5.D (5): Page size: to fit a 640 x 480 monitor
Major links and search button should appear immediately (i.e., no need to scroll to see the main links).

94.5.D (6): Search option:
Searching is best implemented by using the HTML Forms feature, defined as part of the Level 2 specification. Pressing the search button passes the text in the entry field on to the search program, which then returns the result of the search, usually displayed as a hypertext selection list.

94.5.D (7): Audio: none

94.5.D (8): Disclaimer: not needed on home page

94.5.D (9): Review of home pages: at least annually

94.5.D (10) Suggestions for Creating GIF Files

94.5.D (10).a: Software: Windows graphics software such as CorelDraw, Freelance for Windows, PhotoShop, and PhotoStyler produce artwork that can be captured with programs such as PaintShop Pro and saved as GIF files.

94.5.D (10).b: Colors: Blue, cyan, magenta, yellow, green, or black work better than pastels or mixed (dithered) colors.

These colors also work well for gradient fills (e.g., radial fill from black to blue).

The 11/8/94 meeting of the EIS passed a policy that CDC and ATSDR would appear jointly on the Mosaic Home Page and be treated as one organization.

95.1: FTP Required Files

At the 4/495 meeting the Standards Committee, at the request of IRMO adopted the following Standards and Guidelines concerning FTP support Files:

95.1.A: README.TXT File Text:

Welcome to the Centers for Disease Control and Prevention and Agency for Toxic Substances and Disease Registry FTP server. Information maintained on this server is in the public domain and is available at anytime for your use. CDC/ATSDR requests that you provide a valid e-mail address when responding to the FTP server's password prompt.

FTP Policy

CDC/ATSDR's file structure is designed to make information easily accessible for faster response. All FTP directories and sub-directories contain the following files:

README.TXT	Contains General Information and Disclaimer Text (ASCII)
INDEX.TXT	Provides a description of file and sub- directories content contained in that directory. Information is presented by file or sub-directory name, date of last update, and description of content. (ASCII)

To maintain information integrity and assure system security, anonymous uploads ARE NOT ALLOWED.

Comments

Please send general comments or to report any problems experienced while accessing this archive, to: netinfo@address. Also, for your convenience, a contact address for comments or questions specific to information or file is provided in the topical directory README file.

Statement of Authenticity

This material has been cleared for public distribution by CDC/ATSDR and will be authentic if obtained directly from ftp.cdc.gov. CDC/ATSDR takes all effort to assure the authencity of electronically distributed documents. However, in all instances where the electronic and official agency record differ, the authenticity of the official agency record is controlling.

95.1B: INDEX.TXT File Text:

The following items are available in the ftp.cdc.gov pub directory:

Directory/ File Name	File Size	Date of Last Update	Description of Content

95.1.C Some Suggested Guidelines:

95.1.C (1): The download transfer method be added as a column in INDEX.TXT. The committee identified two download transfer methods: Binary and ASCII, though more may exist unknown to us.

95.1.C (2): Those posting information to the ftp server be allowed to add information to the README.TXT file concerning general information about the posted files.

95.1.C (3): The directory specific README.TXT file contain standard language regarding file extension used and that the file extensions be standardized. As examples he cited ZIP files for those containing compressed data, accessible thorough programs like PKUNZIP, PDF files for those containing material that requires Adobe Acrobat as a viewer, and WPF for Word Perfect files.

95.2 Commonality of Standards

At the 4/4/95 meeting the Standards Committee approved the following standard concerning the use of standards across various Internet services:

> The similar nature of various aspects of CDC's Internet Services, both present and anticipated, implies that Standards developed for one specific service will be in effect for other services having equivalent functions.

95.4: Information Requests:

At the 4/4/95, and modified for grammar 5/8/95, the Standards Committee accepted the following report of the Information Request subcommittee for Standards and Guidelines concerning information requests:

> Providing health information to the public and the public health community is an important part of CDC's mission. Increasingly, CDC is providing electronic information using communication tools such as the Internet. An effort is underway to develop and present news, publications, data, resources, and general information using the Internet's Wide World Web with multi-media capabilities. This information can be accessed by anyone, anywhere in the world, who has Internet access. Although this access will generate interest in public health issues, it will also generate questions and new requests for information. CDC must be prepared to handle these inquiries with appropriate and standardized responses.
>
> The CDC Internet Standards Committee is proposing standards and guidelines for routing requests to the most appropriate resource and minimizing the impact on staff time.
>
> **95.4.A: Approved Standards:**
>
> 95.4.A (1): Each Agency or CIO home page should have at least one Internet mailbox where questions and comments on technical and content issues can be sent.
>
> *Local mailboxes will encourage general questions and comments to go to the organization responsible for that page's development and maintenance.*
>
> **95.4.A (2):** Generic names for mailboxes should be used rather than personal identifiers. For example, the generic mailbox for the main CDC home page is Anetinfo@cdc1.em.cdc.gov@.
>
> *Generic names will provide continuity in the event of staff changes and protect individual staff members from the impact of controversial issues.*
>
> **95.4.A (3):** When programmatic requests for information come to the CDC front page mailbox, these requests should be sent to the Office of Public Inquiries. This office will then refer the requests to the correct resource. When the request falls under the jurisdiction of FOIA then the Office of Public Inquiries would refer it to the FOIA coordinator. When FOIA requests come directly to a program, the FOIA coordinator should be

notified so that the request can be tracked. Each agency or CIO should develop policies and procedures for handling requests for information that come directly to the agency or CIO or directly to a program.

95.4.B: Approved Guidelines:

95.4.B (1): Include as much information on-line as possible.

95.4.B (2): Include ordering information for information and publications that are available but not on-line.

95.4.B (3): Include references to high volume request topics on the main home page. For example, a "Traveler's Health" topic might be a front page selection, and a section on current topics might be included under a news and current events topic.

95.4.B (4): Use Frequently Asked Questions (FAQs) whenever possible to provide answers to the common questions. FAQs also serve to standardize answers.

95.4.B (5): Include a topic on the main home page that references other information sources such as the VIS, the AIDS Hotline, and other Web servers.

95.5: CDC Newsgroup Subscriptions

At the 6/12 meeting of the Internet Standards Committee the following standard for CDC subscription to existing newsgroup was passed for Steering Committee review:

CDC/ATSDR Newsgroups subscriptions are added to the CDC/ATSDR system by specific request through the C/I/O IRM Coordinator to the CDC Information Center, after which they become available for use. That request must contain:

the Newsgroup name,
the business reason for subscribing to the Newsgroup,
the person or group within the C/I/O requesting the subscription, and
limitations on who within CDC/ATSDR can use the Newsgroup, if applicable,

and the person responsible for determining this status.

If the request does not include limitations of access then the C/I/O IRM Coordinator is responsible for specifying if any limitations should apply.

The Internet Technical Staff will subscribe to any Newsgroup requested if all the above information is provided and the subscription is technically feasible. If the subscription is not technically feasible, the person or group within the C/I/O must be notified of reason.

A current list of Newsgroups subscribed to by CDC/ATSDR will be maintained and accessible within CDC/ATSDR from the World Wide Web Home Page. The list will contain the name the Newsgroup, any access limitations, and the person or group within the C/I/O responsible for the subscription.

95.6: External Use of "cdc.gov "

The following standard was passed by the committee at the 7/10 meeting:

> A Project Director may provide either links or resources to project specific Internet Resources at the expense of the project. If these Internet Resources have as part of their address any form of the traditional "cdc.gov" Internet address and the information placed in those resources does not go through the formal CDC clearance process, as might be the case if the project provides resources for a state agency or private foundation, then the resources must have the following disclaimer at the opening of the resource:
>
> "This space is provided by CDC to (agency maintaining this information). Information and views presented are not that of CDC but that of (agency maintaining this information)."

96.1: Establishing Routine and Special Internet Services

The following was approved by the Internet Steering Committee at the 9/5/96 meeting:

96.1.A: Introduction

IRMO provides for CDC/ATSDR a set of basic Internet services readily available to all. In addition, many projects at CDC/ATSDR require special Internet services beyond what is required by the general user. While not absolute, the basic services are only available outside the firewall and do not have the potential to interact with the CDC Wide Area Network (WAN). Special services generally cross the firewall and have the potential to interact with the CDC WAN.

Examples of special services include, but are not limited to transfer of files from the outside to CDC/ATSDR (FTP) and remote operation of CDC/ATSDR computers (TELNET). CDC/ATSDR has chosen to distribute Internet services directly over our existing WAN and free introduction of these services represent a security problem that must not be ignored. We must also not ignore that projects require these special services to operate. IRMO has and is acquiring the tools to allow free distribution of general Internet services to all and also the tools to allow easy introduction of special services to those that require them.

The standard proposed below provides a mechanism for listing and requesting both basic and special services. It also outlines the requirements of the requester and IRMO in providing these services. The introduction of the proposed standard would make the requests for both basic and special Internet services a routine function of IRMO, equivalent to the requests for routine and special services on the mainframe.

96.1.B: Approved Standard

> **96.1.B (1):** CDC/ATSDR provides basic services to all users who have Internet access. The Information Resources Management Office (IRMO) shall periodically, at least annually, provide to the Center/Institute/ Office (C/I/O) Information Resource Management (IRM) Coordinators a list of services they consider part of the basic operation of our Internet services, the mechanism an IRM Coordinator can use to request those services, and support IRMO provides for that service. Requests for new basic level services must be approved by the Internet Provider's Committee. Request for deletion of a basic Internet service must be approved by both the Internet Provider's Committee and the IRM Coordinators.
>
> **96.1.B (2):** The basic service set, like the basic mainframe services, meet the needs of most users. Some users, however, have needs for services not provided by the basic set found on the current list provided by IRMO. These unlisted services are considered Special Internet Services. Based on observations from other Internet sites, we assume that these special services can be provided, in some fashion, without compromising the

integrity of our existing services.

96.1.B (3): IRMO shall maintain the hardware and software infrastructure required for all CDC/ATSDR basic services. IRMO may require that a project provide supplemental hardware and software if the request for basic services is of unusual complexity, size, or location. Except as noted below for special service requests that result in new basic services, the project shall provide all additional hardware and software required for a special service request. Excepting those services provided on IRMO supported hardware, the project is responsible for all basic and special support costs. For both basic and special services, the project is always responsible for maintenance of the internal structure, such as membership lists and material, of Internet services.

96.1.B (4): Requests for special Internet services are made by specific request through the C/I/O IRM Coordinator to the IRMO Network Technology Branch (NTB), after which they become available for use by those requesting the service. That request must contain:

1. the specific service requested including, if applicable Internet Socket Service by name or number and any point-to-point IP address connection information,
2. the programmatic reason for requesting the service,
3. the length of time the service is desired (maximum of two years - renewable),
4. the person or group within the C/I/O requesting the service,
5. limitations on who within CDC/ATSDR can use the service, including, if applicable, IP addresses, and the person within the program responsible for maintaining the service.

96.1.B (5): In reviewing the request for special Internet services, the IRM Coordinator must consider if the service request involves any items in addition to those noted above, and assess the potential impact on the security of the CDC Wide Area Network (WAN). They should also determine if the requester has informed the outside party of CDC's security requirements and, if not, contact the outside party and supply them with the current written description of their security requirements. IRMO shall maintain and make available the security requirements for outside partners. Once the IRM Coordinator is satisfied the requester has meet all requirements they will forward the request to IRMO NTB.

96.1.B (6): IRMO NTB will implement any valid special service request that is complete, technically feasible (given existing resources) and does not represent an unreasonable risk to the CDC WAN. They will advise the requester if the task can not be completed within five working days or if unusual security implications exist.

96.1.B (7): Any special service request that IRMO NTB determines is incomplete or represents an unreasonable security risk will be returned to the C/I/O IRM Coordinator within five working days of the request with asking for the specific missing information

or modifications. If the request represents an unreasonable security risk, the CDC/ATSDR Information System Security Officer (ISSO) must also be notified.

96.1.B (8): Any special service request that is found not technically feasible given existing resources is automatically forwarded to the Internet Technical Committee for review. The Internet Technical Committee shall review the request and advise the IRMO NTB if resources should be expanded to provide the service and if the cost of the expansion is in the general interest of CDC/ATSDR. If the special service requires expansion of resources (either equipment, software, or personnel) the request then becomes part of the normal budget process. The requester of the service will be informed of the results of this review through the C/I/O IRM Coordinator.

96.1.B (9): IRMO NTB will immediately inform the requesting C/I/O IRM Coordinator of a request forwarded to the Internet Technical Committee or the ISSO. The C/I/O IRM Coordinator or designee will then work with the Internet Technology Committee or ISSO until a resolution of the technical or security issue is reached.

96.1.B (10): For any special service requested for greater than six months, the requester of the special service will receive notification of pending termination of that service at least one month prior to termination.

96.1.B (11): IRMO shall have plans in place for the automatic and orderly restoration of special services in the case of system failure.

96.1.B (12): IRMO shall advise any requester of special services of any technical changes in Internet Services that will adversely affect the special service at least one month before the change becomes effective.

96.1.B (13): IRMO and the ISSO shall periodically and at least annually review the extent of Special Internet Services and provide an assessment of the security risk to the CDC WAN to the Internet Steering Committee.

96.2: Sponsored Discussion Forums

96.2.A: Rationale:
Internet discussion forums allow CDC/ATSDR and the public exchange information and ideas that allow us to achieve our goal of strengthening the public health infrastructure. The creation of discussion forums will effectively exchange CDC's vast public health knowledge and expedite the interaction and networking that truly defines a productive electronic community. Newsgroups (topic specific question and answers sessions), and LISTSERVers (general E-mail distribution and response systems) are the primary means used on the Internet as discussion forums. New methods, such as web conferences are emerging totals that serve similar purposes.

Internet discussion forums exist in two forms: Moderated and Unmoderated. A Moderated discussion forum has all material screened before posting. An Unmoderated discussion forum has no material screened before posting. Moderated discussion forums are a potential problem because they will require an editor to review all information. That editor may choose to re-word some of the posting or even not post some information. A Moderated discussion forum is very successful when working with a specific, generally technical, subject. People joining the discussion forum can feel they are getting useful, specific information on the topic. As editing is involved, a time requirement for the program sponsoring the material is needed, which could be difficult for those with limited budgets or staff. Also the issue of censorship can arise. As long as participants are aware editing will occur and that the type of editing is defined, it is permitted under CDC policy.

An Unmoderated discussion forum has little time requirements from the program as all responses are posted. The problem with this type of discussion forum is that material can be posted from the outside that could be consider abusive or, if phrased properly, might be considered an official viewpoint. This type of discussion forum is helpful when dealing with issues of concern to the general public. Participants are to be made aware the forum is Unmoderated and could contain information not approved by CDC/ATSDR.

Internet has a body that controls official Internet Newsgroups (USENET). After reviewing the requirements for establishing on official USENET Newsgroup, it was felt that many of our topics would be of narrow interest and could not pass the USENET voting requirements. Also, the time spent (three to six months) having a Newsgroup approved by USENET was burdensome. It was decide for CDC/ATSDR to operate only private Newsgroups, not approved by USENET. The major problem that arises from this discussion is that we would not formally have replication sites for our Newsgroups and most users would have to contact the CDC/ATSDR Newsgroup Server directly. USENET Newsgroups are automatically upgraded at replication sites throughout Internet.

96.2.B: Approved Standard:

96.2.B (1): CDC/ATSDR C/I/O's may sponsor discussion forums on Internet on public-health related topics if such activity will further CDC's and ATSDR's missions that originate from and/or are located on the CDC/ATSDR Internet Server(s). Those discussion forums will adhere to the standard proscribed herein. These standards do not apply to CDC sponsored discussion forums that originate from and are located on servers different from those used by CDC.

"CDC/ATSDR-sponsored discussion forums" include Internet newsgroups, LISTSERVers, and other similar Internet discussion formats now existing or to be developed, such as Web Conferences, established by CDC/ATSDR or by organizations outside of CDC/ATSDR with CDC/ATSDR funding or support. In the specific case of newsgroups, these are not part of the official Internet newsgroups ("USENET") but use the same Internet protocol (Network News Transport Protocol [NNTP]).

CDC/ATSDR-sponsored discussion forums may have enrollment, where enrollment indicates the ability to submit information to the discussion forum, open to the public ("public discussion forums") or be closed with enrollment restricted to selected groups or individuals ("private discussion forums"). The justification and criteria for restricting private discussion forums must be clearly stated. CDC/ATSDR discussion forums will not place any restrictions on public viewing of information.

96.2.B (2): CDC/ATSDR-sponsored discussion forums may be "moderated", that is, material contributed by participants is reviewed before posting, or "unmoderated" (not reviewed). The purpose of the discussion forum and the degree to which submissions are reviewed must be clearly stated to all users.

96.2.B (3): If a CDC/ATSDR-sponsored discussion forum is moderated (reviewed), the criteria for review must be clearly stated to all users. These might include relevance to the discussion forum's stated purpose, courteous wording, and absence of profanity and provision of name and institutional affiliation. The criteria may not exclude free expression of opinion, even if counter to that of CDC/ATSDR. It is recommended that errors of fact, where differences of opinion may exist, be pointed out in related messages rather than excluded.

Each CDC/ATSDR-sponsored discussion forum (public or private) must have a designated person who would:

(a) Act as the moderator in a moderated discussion forum,

(b) Periodically post to the discussion forum:
- the purpose of the discussion forum
- whether the discussion forum is public or private, and justification for this designation
- criteria for participation in private discussion forum
- whether the discussion forum is moderated, and the criteria for excluding material

- frequently asked questions (FAQ's) concerning the discussion forum

Information posted to the discussion forum should be archived and treated as electronic government records.

96.2.B (4): CDC/ATSDR staff participating in discussion forums of whatever sponsorship should adhere to the standards to be developed for electronic mail issued separately. Until such time as that policy is formally adapted, participants in electronic forums should take care when posting original or response material to indicate either implicitly or explicitly that the material represents their personal views and not CDC policy. Postings containing CDC policy should explicitly indicate that the posting does contain approved policy.

96.2.B (5): Programs should submit requests for establishing a CDC/ATSDR sponsored discussion forum are first approved through the C/I/O Director, who, in the case of a public unmoderated discussion forum, must indicate why that forum must exist on a CDC server and cannot be placed on one sponsored by, but external to CDC. After C/I/O Director approval, the request continues through the C/I/O IRM Coordinator to the Information Resources Management Office (IRMO) Network Technology Branch, after which they become available for use. That request must contain:

(a) a brief description of the discussion forum including:
- name of the discussion forum
- type of discussion forum (newsgroup, LISTSERVer, web conference, etc.)
- focus of the discussion forum,
- if it is moderated or unmoderated,
- if unmoderated and public the C/I/O reasons for placing it on the CDC server,
- if moderated, the review criteria
- requesting organization name
- date required to be on-line, and
- intended audience

(b) the programmatic reason for requesting the discussion forum, the person or group within the C/I/O charged with maintaining the discussion forum.

The IRMO Network Technology Branch will implement any valid discussion forum on the appropriate CDC Server so long as the request that is complete and technically feasible (given existing resources) and advise the requester when the service is available to the public. If the request is not granted for technical reasons, IRMO shall notify the program when they will be able to supply the required technical resources and establish the discussion forum on or about that date.

97.1: CDC Internet Access Policy

97.1.A: Rational:
The Internet Standards Committee was asked early in its history to draft a proposed policy for access by CDC employees to the Internet. During the development of this policy, the Department indicated they would be developing universal Internet Access policies. A draft of those policies was produced, but a decision was made to release them as just recommendations. This draft policy uses those recommendations as the basis for the CDC policy for employee Internet Access.

The key feature of the DHHS draft access policy was universal access by all employees, though not necessary at each workstation. A second feature was the ability to use the Internet connection for limited, non-work related information access, provided no additional cost was incurred. DHHS felt that limited non-work related access would help develop Internet use skills that were directly transferable to the workplace. A third feature was the requirement for each agency to have an Internet address.

The following draft policy incorporates these concepts. It also adds the requirement that each CIO have a unique Internet address and state it on their home page.

97.1.B: Accepted Policy (5/15/97):

97.1.B (1): CDC/ATSDR employees shall be provided with access to Internet services in order to obtain and exchange information in conformance with the general requirements of their government responsibilities. Such services shall include all basic CDC/ATSDR Internet services they may require to the extent and in the manner authorized by CDC/ATSDR Internet policies, standards and procedures. Access may be through an individual's workstation or conveniently located central workstations available for general use.

97.1.B (2): Internet addresses shall be distributed by organization. Each Center/Institute/Office shall have its own mailbox, identified on a home page.

97.1.B (3): Internet use is limited to activities that support the CDC/ATSDR missions. Unacceptable uses include, but are not limited to, unlawful or other malicious activities prohibited on Federal property; misrepresentation of oneself or CDC/ATSDR and activities that could cause congestion and disruption of networks and systems.

97.1.B (4): CDC/ATSDR permits staff to use the Internet for educational purposes in order to practice Internet skills and explore Internet resources provided such use occurs during non-work time while at their normal work site and does not incur any direct additional charges (i.e.; does not use services for which there are charges on either a time or usage basis).

97.1.B (5): Employees should also be aware that they have no expectation of privacy while using any Government provided access to the Internet. The CDC/ATSDR views electronic mail messages to be Government records, and it may have access to those messages whenever it has a legitimate Governmental purpose for doing so. Please also remember that all Internet communications identify the user to all sites accessed. Specifically, the sender is identified by his or her complete Internet address, including the "cdc.gov" domain."

97.2: Repeal of Home Page Style Standard

The Internet Home Page Standard was repealed by the Internet Steering Committee 7/97.

Action:
The existing Home Page Standard (94.5) is repealed. By agreement, that standard has not been enforced for over a year, until a new standard was developed. Experience with Internet has shown that any style standard would outdate shortly. Common sense and usage experience have proven a successful style guide. With that in mind, we recommend no replacement standard.

97.3: Internet Page Information/Style Standard

The Internet Style Standard was adopted by the Internet Steering Committee 7/97.

97.3.A: Rationale:
After two years of experience in using Internet, the Standards Committee desires to codify a simple set of standards for information and style of pages that appear as part of our Internet site. Information noted as required has proven to be useful and currently exists on most, if not all pages. Style guidelines are presented to make navigation easier, especially when entering in the middle of a CIO page, as can happen from an external search. Other style guides make searching easier and provide usable information for people with disabilities.

97.3.B: Standard:

97.3.B (1): All external links should be clearly identified as such. Whenever possible these links should be grouped together. Otherwise, the context should clearly indicate that the link is external to CDC.

97.3.B (2): Each Agency or CIO home page should have a navigational link back to the CDC home page. Internal, within CIO, navigational pages should have links to the CDC and/or CIO home page. All other pages should have navigational links when possible.

97.3.B (3): Each page should have the HTML TITLE attribute to provide information for a search listing. Other indexing attributes are encouraged so long as they increase the chances for significant information to be found.

97.3.B (4): Pages should have text equivalents to be in compliance with the Americans With Disabilities Act (ADA). Pages that make heavy use of tabular material or require a PDF format, such as MMWR, are not required, but are encouraged, to have text equivalents.

97.3.B (5): Each Agency or CIO home page should have at least one Internet mailbox. (Refer to the standard on Information Requests.)

97.3.B (6): Home pages and other information published on the Internet should go through the CIO's designated clearance procedure.

97.3.C: Guidelines:

97.3.C (1): Authors of HTML pages should make an effort to include either a header or footer on each page that indicates the material is from CDC.

97.3.C (2): Authors of HTML pages should make an effort to use common images across all pages. IRMO maintains a directory of useful images that should be consulted before creating your own image.

98.1A: Policy for Secure Internet Exchange of Information

The Policy for Secure Internet Exchange of Information was approved by the Internet Steering Committee and the Health Information Surveillance Systems Board (HISSB) on 4/9/98 after external review.

98.1A: Changes as a result of the first annual review of the policy by the CDC ISSO as accepted by the Internet Steering Committee (4/8/99) and subsequent acceptance by HISSB.

98.1A.A: Issue and Need:

Growing use of the Internet by both the public and private sector is rapidly making network an important medium for information exchange. While the Internet allows for easy connectivity, such ease is counterbalanced by inherent issues concerning the ability to protect the privacy and integrity of information and to ensure that information is accessible only by those for whom it was intended.

Information and data can be transmitted over the Internet -- and other media -- by connecting to servers through various protocols such as FTP (File Transfer Protocol) and HTTP (Hyper Text Transfer Protocol), as an E-mail message or attachment, or by connecting to a system as a remote user. Without adequate protection, information transmitted over the Internet does not inherently possess any assurance that the information actually originated from the indicated source (addresses may be spoofed), that it has been viewed only by intended parties (information might be intercepted either during transmission or from an intrusion on the local or remote systems), or that it has remained unchanged during transmission. In order to define appropriate security controls, the information must be categorized according to the potential harm associated with its loss, alteration or disclosure. The information can be protected by the appropriate use of security controls, including encryption, authentication, integrity verification, and assurance of non-repudiation applied to the transmission process.

There is a need for general rules of operation that will allow our programs and programs we sponsor with our partners to use the Internet as a communication medium. Policies are needed for information exchange via the Internet which address risk analysis for sensitivity and criticality, security control requirements, and audit/verification procedures.

98.1A.B: Scope of Policy:

This policy applies to three unique, but somewhat overlapping, areas:

1. Electronic transmission of information;
2. Electronic Mail (E-mail);
3. Remote Access

This policy will address the electronic transmission of information using protocols such as FTP, HTTP, and E-mail. Although the possibility of loss, alteration, or compromise of confidentiality may differ between these methods of information transmission, for the purposes of this document, they can be treated the same.

This policy does not address the establishment, documentation or maintenance of the integrity, authenticity or trustworthiness of information sent and/or received and the encryption keys used in this process. CDC/ATSDR policy documents that address these issues need to be developed and enacted. Also, though not specifically addressed in this policy, many of the methods and principles noted can also be applied to non-Internet-based communication.

98.1A.C: Policy:
(Note: See Section IV below for specific definitions of terms used.)

98.1A.C (1): Agency annual review:

> The CDC/ATSDR Information Systems Security Officer (ISSO) shall, at least annually, review the overall policy for Internet Exchange of Information, as stated in the Terminology and Security Levels sections of this policy, and submit any recommendations for changes to the Internet Standards Committee for consideration and adaptation through the standard process. In preparing these recommendations, the ISSO shall seek and consider any recommendations from the Excellence in Science Committee or the Health Information and Surveillance System Board (HISSB), as well as input from ATSDR, CIOs and our partners.

98.1A.C (2): CIO and ATSDR defined procedures:

> Each CIO and ATSDR shall define procedures for assigning security levels and for internal review of the security level. The Business Steward for a program will assign the security level with review by the CIO or ATSDR ISSO. The CIO or ATSDR procedures for Secure Internet Exchange of Information must comply with the terms of the policy set forth in this document.

98.1A.C (3): Program security plans:

> Every program requesting the use of the Internet for exchange of information with a high level of sensitivity and criticality must have as part of its overall security plan a section addressing information exchange that is program specific, uses the standard CIO security plan, or uses the standard CDC/ATSDR security plan for information with a high level of sensitivity and criticality. Each program must state specifically which plan they are using. If

they are developing a program specific plan, the approval process should include the CIO ISSO and the CDC/ATSDR ISSO.

98.1A.C (4): Agency resource requirements:

CDC/ATSDR shall operate through Information Resources Management Office (IRMO), with the collaboration of the ISSO, an Internet connection and security gateway facility capable of receiving and transmitting information that has a high level of sensitivity and/or criticality. CDC/ATSDR shall maintain, through IRMO and the ISSO, a standard set of security systems including specific software, hardware, and policies of access and use. Wherever possible, the standard sets should use industry standard specifications and tools. CDC/ATSDR shall provide adequate and appropriate training for the software, hardware and tools.

98.1A.C (5): Program resource requirements:

98.1A,C.i: When considering the use of Internet as a transfer medium for information that has a high level of sensitivity and/or criticality, programs should analyze and be responsible for external and internal resource requirements for additional security systems. When security systems are required to be implemented in partner sites, programs must also consider the impact on personnel and resources at those sites.

98.1A.C.ii: After a date to be determined by the HISSB, CDC/ATSDR programs are required to use the above secure facility for transmission of all high sensitivity/criticality data unless specific written authorization to use an equivalent or more secure facility is obtained from the CDC ISSO in consultation with the ATSDR/CIO ISSO.

98.1A.C.iii: Program's specific security plans will conform to this policy. All secure systems that do not use the standard set of security systems must be registered with the CDC ISSO and the ATSDR/CIO ISSO. Where consensus can not be reached on proposed exemptions, these shall be appealed to the HISSB. The following must be disclosed to the CDC ISSO, ATSDR/CIO ISSO and IRMO as indicated below:

1) When planning to use an alternative Internet security mechanism, registration shall be within 15 days of authorizing the planning effort;
2) When undertaking development of an alternative Internet security mechanism, registration shall be no later than 15 days after the first development meeting;

3) When procuring hardware, software or services to develop or implement an alternative Internet security mechanism, registration shall be no later than 30 days before the expected procurement action..

98.1A.D Other Sections: Terminology and Security Levels:

98.1A.D (1): Terminology:

Terms used in this policy are known to have several commonly understood interpretations. Hence, for the purpose of this policy, the following descriptions and definitions apply:

Authentication — A process to uniquely identify the entity requesting access to or submitting information. Authentication methods are part of both the security system and confidentially rules. For computer information, authentication procedures must account not only for potential human access, but computer-to-computer generated requests for information as well.

Public key encryption systems provide authentication with digital signatures. Digital signatures verify that information has not changed since someone signed it, and they give the recipient a way of verifying who signed it. It would be very difficult for a compromised file (i.e., a file that has been tampered with) to duplicate the original checksum value.

Confidentiality — The condition of preserving distribution of, or access to, information according to requirements of law, custom, the desires of the object of the information, or of the owner of the information.

Confidentiality is most often preserved by adhering to standard rules of behavior that specify how access to and use of private information will be regulated. These rules should be written and, for computer systems, be expressed and enforced through access control software.

Confidentiality should be provable, requiring a trusted and complete audit trail, to the level required and is available for review. Where appropriate, the audit trail should indicate the identity of all who had access to the information, the date and time of such access, the mechanism by which access was gained, and whether any portion was copied or altered. A properly constituted system which processes confidential information will allow access

to information only by those who are duly authorized and will fully document that access.

Criticality — Systems are critical to the degree that lack of access to the functions provided by the system, the data which are manipulated by the system, or the products of the system impede or block the agency from fulfilling its overall mission.

Encryption — Encryption is defined as precisely encoding information so that only parties intended to view the information can do so.

There are many ways to encrypt information, and the most commonly available systems involve public key and symmetric key cryptography. A public key system uses a mathematically paired set of keys, a public key and a private key. Information encrypted with a public key can only be decrypted with the corresponding private key, and vice versa. Therefore, you can safely publish the public key, so that anyone can encrypt a message that can be read only by the holder of the secret key. Presuming that the secret key is known only to the one authorized individual, a message is then accessible only to that one individual. A symmetric key system is based on a single secret key which is shared between parties. Symmetric systems require that keys be transmitted and held securely in order to be effective, but are considered to be highly effective when the procedures are good and the number of individuals who possess the key is small. In general, under both systems, the larger the key, the more robust the protection.

Firewall — A barrier between two environments which is designed to allow interchange across the barrier according to specified rules.

Most often, a firewall is thought of as the barrier between a publicly accessible computer domain, such as the Internet, and a private one, such as the CDC-Net which only serves CDC and ATSDR. A firewall, however, can be used within a large private computer domain to more clearly define and enforce the business rules on communication between parts of the same corporate structure.

The physical implementation of firewalls can vary. Some are simply a router with a carefully crafted routing table. Others are specialized programs running on a dedicated machine. Still others are hybrids. No firewall implementation ought to be considered completely secure by itself, and the protection expected from the

	firewall needs to be clearly defined as part of an overall information protection and systems security program.
Integrity	A quality of information that represents the degree to which it (a) reflects the reality it was intended to, (b) has been protected from unauthorized, unanticipated, or unintentional modification, and (c) captures all authorized changes and, when appropriate, all access -- including detection of unauthorized activities. A quality of a computerized system that represents the degree to which the combination of hardware, software and communications behave predictably and reliably within the actual expected operating conditions and the degree to which the combination does not change through other than authorized procedures.
Non-repudiation	A state when it is virtually impossible for the individual or party identified as the sender to repudiate the message, that is: to claim successfully that either someone else sent the message or that the content of the sent message was different from the received message. Agreements for electronic exchange of information are normally entered into via formal written mechanisms, where the rules are spelled out and there is mutual acceptance of legal standing of all document transmitted under the agreement. To be complete, these rules must cover the expected behavior regarding authentication of the user of such a system to that individual's internal system, particularly in regard to sharing of ID/password pairs or other means of electronic verification of identity. To insure non-repudiation, the electronic text or file is "signed" using a digital signature mechanism which assures, to a very high degree of probability, that the identity of the sender is actually that of the person identified within the message as having been the sender and that the content of the message has not changed.
Privacy	The condition of having control over which information about oneself, either as an individual or as a recognized entity, is shared with another party. Our legal system acknowledges an inherent right of an entity to keep information from others. An individual’s perception of a right to privacy may be based on law or custom, or may be simply a projection of the individual’s desire.

	Information which is acknowledged in law or custom to be private may be used by others without fear of penalty under specific legally accepted terms, as is commonly done in the field of public health. In a subset of such situations, the information may be used without the express permission of the enity. Except where permitted by law, use of information without the consent of the owner is unacceptable.
Security	The preservation of integrity, authenticity, availability and confidentiality of both systems and the information created, stored, manipulated, received or transmitted by such systems.
Security Level	A summary indicator of the amount of protection required for the information and system(s), based on the sensitivity and criticality of the information and systems. Security level and cost are two of the principal determinants in selecting protective measures, which can include administrative procedures, auditing, use of encryption and sophisticated electronic authentication procedures.
Sensitivity	Sensitive data are those that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction or from inappropriate creation. Sensitive data include those whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, data collected under the Public Health Service Act Sections 301(d) and 308(d), and data withheld from release under the Freedom of Information Act. Sensitive systems are those which process sensitive data or pose a significant risk and magnitude of loss or harm from improper operation, deliberate manipulation, or delivery interruption.

98.1A.D (2): Security Levels:

Low	Information that has no real or perceived privacy requirements and poses no threat to individuals, corporate entities or the agency. This level requires neither security rules nor special security requirements. Information rated as low security level may be sent in an unsecured manner such as clear text in an e-mail message, as

an unencoded attachment, or from a web entry form located on an unsecured server. An example of low risk information is that placed for public access on our World Wide Web site. Also, material that has CDC Clearance inherently has a low level of risk. One caveat is that, in the electronic age, we must assure that such publicly accessible data have not been altered maliciously.

High

Information that has real or perceived privacy requirements as viewed by the general public and poses a high level of threat to individuals, corporate entities or the agency. Security rules for this type of information must provide extensive protection and include at least:

- protection of the information by encryption with public key technology using keys of at least 128 bits in length;
- storage of information only in encrypted form outside the firewall;
- transfer of the information from outside to inside the firewall in a minimal, defined period;
- removal of the information from outside the firewall immediately after verification of a successful transfer;
- unique authentication information contained in the transferred file to indicate it originated from the specified source and is in the unaltered original form;
- a connection authentication system that requires at least two levels of connection control such as server log in and certificate authentication;
- a full audit trail of all connections and entities originating the connections; and
- a limited, defined set of entities that can use the external system.

When unique, personal identification information is included, it is further recommended that additional steps be taken to remove the identifying information before transmission and provide alternative linkage mechanisms for research purposes.

Information with a high level of sensitivity and criticality may also be sent as an E-mail attachment provided it meets the above encryption requirements and the receiver has a way of authenticating the sender other than by the E-mail address. The unencrypted information must never be placed on an E-mail server or on any system with external visibility. Use of encrypted E-mail for ongoing or repetitive programmatic data transfer shall be an alternative approach requiring approval as detailed above.

The primary example of this type of information is surveillance data containing personal identifiers. It will also apply to any information used by a project having protection under Section 308(d) or 301(d) of the Public Health Service Act (42 USC 242m) and will most likely apply to any raw data transferred externally on projects requiring approval by Institutional Review Boards.